Amendments to the Claims

Claim 1 (currently amended): A computer-implemented method of achieving context-sensitive confidentiality among security domains within a federated environment that spans a plurality of security domains, the method comprising ~~steps of~~:

determining a route to be taken by a content request message to be transmitted from a content requester in the federated environment to a content provider in the federated environment, [[where]] wherein:

the route comprises a network transmission path which begins at the content requester and ends at the content provider and passes through a plurality of intermediary nodes, each of the intermediary nodes located between the content requester and the content provider on the network transmission path;

the route is determined by consulting stored policy that specifies, for the content receiver sending the content request message to the content provider, the network transmission path; and

the route spans a plurality of the security domains;

storing the determined route at a network-accessible location;

determining, prior to transmitting the content request message from the content requester, a plurality of portions of the content request message that are security-sensitive, further comprising using a context to consult stored policy that identifies the security-sensitive portions which are applicable to that context, wherein the context comprises an identification of the content requester, an identification of the content provider, and a message type

identifying the content request message;

determining, prior to transmitting the content request message from the content requester, rights of each of the intermediary nodes ~~to be encountered on the determined route~~ to access each of the determined security-sensitive portions of the content request message, further comprising consulting stored policy for each of the intermediary nodes, wherein the stored policy specifies whether this intermediary node is entitled to access this security-sensitive portion of the content request message;

specifying, in unencrypted form in the content request message, the message type; an identifier of the network-accessible location where the determined route is stored; and a plurality of message receiver elements, wherein a separate one of the message receiver elements is specified for each of the intermediary nodes that is entitled to access each of the security-sensitive portions, the separate one specifying an identification of that intermediary node as a permitted receiver of that security-sensitive portion and a node-specific keyword corresponding to that intermediary node;

selectively protecting the security-sensitive portions of the content request message, according to the determined access rights by encrypting, for each of the security-sensitive portions of the content request message, that security-sensitive portion separately for each distinct one of the intermediary nodes which is entitled to access that security-sensitive portion and storing that separately-encrypted security-sensitive portion in the content request message in association with the node-specific keyword corresponding to that distinct one of the intermediary nodes, thereby enabling each of the intermediary nodes to locate and access each

of the security-sensitive portions which it is entitled to access and preventing that intermediary node from accessing any of the security-sensitive portions which it is not entitled to access; and

transmitting the content request message with its selectively-protected portions from the content requester to the content provider on the determined route, wherein:

the transmitted content request message contains information identifying an authentication authority from a first of the security domains and an identification of a party for which the content request message requests access to services and indicates that the identified authentication authority has already authenticated the party using security credentials of the party in the first security domain;

the intermediary nodes and the content provider, upon receiving the content request message in other ones of the security domains, can bypass authentication of the party for access to services of that other security domain, upon verifying authenticity of the authentication authority, establishing that the authentication authority vouches for the received content request message, and using the identification of the party to locate previously-stored security credentials for the party which are usable within that other security domain; and

the security credentials for the party in at least one of the other security domains are different from the security credentials of the party in the first security domain.

Claim 2 (canceled)

Claim 3 (currently amended): The method according to Claim 1, wherein the selectively

protecting [[step]] further comprises ~~the step of~~ computing a digital signature over at least one of the security-sensitive ~~portion~~ portions of the content request message.

Claims 4 - 5 (canceled)

Claim 6 (currently amended): The method according to Claim 1, further comprising ~~the step of~~ determining a role of at least one of the intermediary nodes ~~to be encountered~~, and wherein ~~the step of~~ determining the access rights further comprises ~~the step of~~ using the determined role when consulting the stored policy ~~for each determined role~~, wherein the stored policy specifies whether nodes in that role are entitled to access this security-sensitive portion of the content request message. ~~access rights for that role.~~

Claim 7 (canceled)

Claim 8 (currently amended): The method according to Claim [[7]] 1, wherein the encrypting step uses a public key associated with each of the intermediary nodes for which the encrypting ~~step~~ operates.

Claims 9 - 11 (canceled)

Claim 12 (currently amended): The method according to Claim 1, further comprising ~~the steps~~

~~of~~:

receiving the transmitted content request message at a selected one of the intermediary nodes on the determined route;

using the identifier of the network-accessible location where the determined route is stored, by the selected one, to locate a next hop for forwarding the content request message from the selected one on the determined route;

locating, by the selected one, each of the separate ones of the message receiver elements that specifies the identification of the selected one and retrieving therefrom the specified node-specific keyword; and

securely accessing only those ones of the selectively-protected portions of the received content request message to which the selected [[node]] one has access rights by using each of the retrieved node-specific keywords to locate and access only those ones of the security-sensitive portions which the selected one is entitled to access.

Claim 13 (canceled)

Claim 14 (currently amended): The method according to Claim [[13]] 1, wherein the authentication authority is determined to vouch for the received content request message if a digital signature computed by the authentication authority and transmitted with the content request message is determined, by the intermediary node or the content provider, upon receiving the content request message in the one of the other security domains, to be valid.

Claim 15 (currently amended): The method according to Claim [[13]] 1, wherein the transmitted content request message contains security credentials of the party, where those security credentials have been authenticated by the identified authentication authority and are protected such that only authorized ones of the intermediary nodes and the content provider, upon receiving the content request message in other ones of the security domains, can access the protected security credentials.

Claims 16 - 21 (canceled)